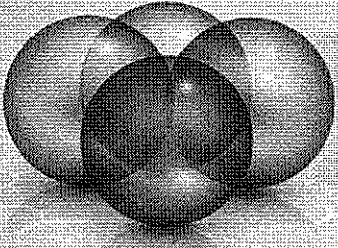


**covisint** | Connect. Engage. Collaborate.



## Cybersecurity Issues within a changing cloud landscape

A briefing for the Michigan State Senate

- David Miller Chief Security Officer


## OUR BACKGROUND

26,000 CUSTOMERS

68,000 SUPPLIER ORGANIZATIONS

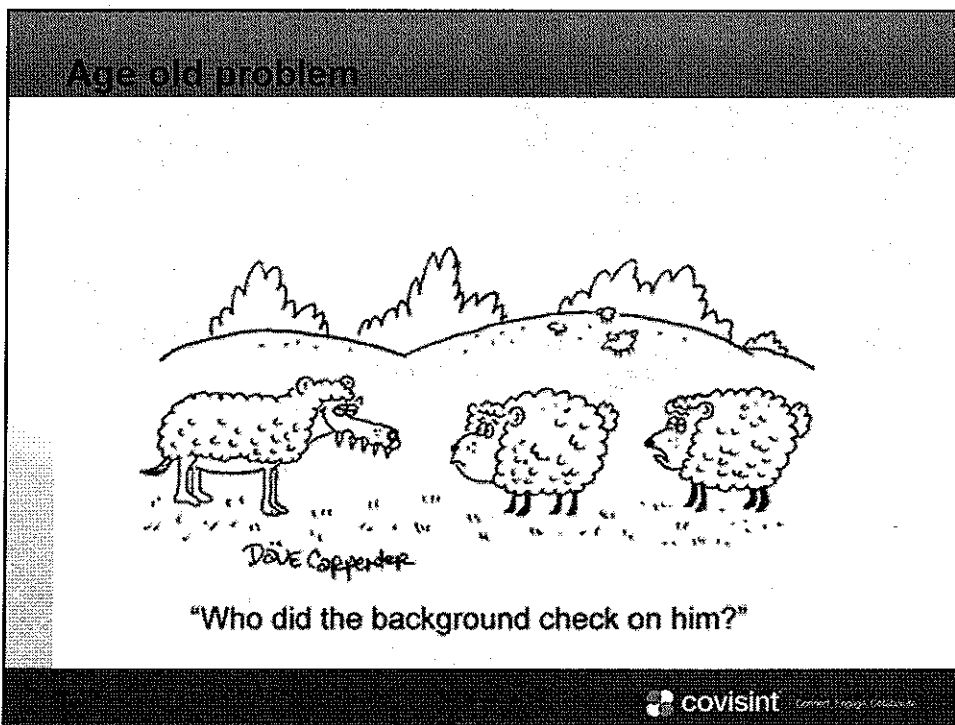
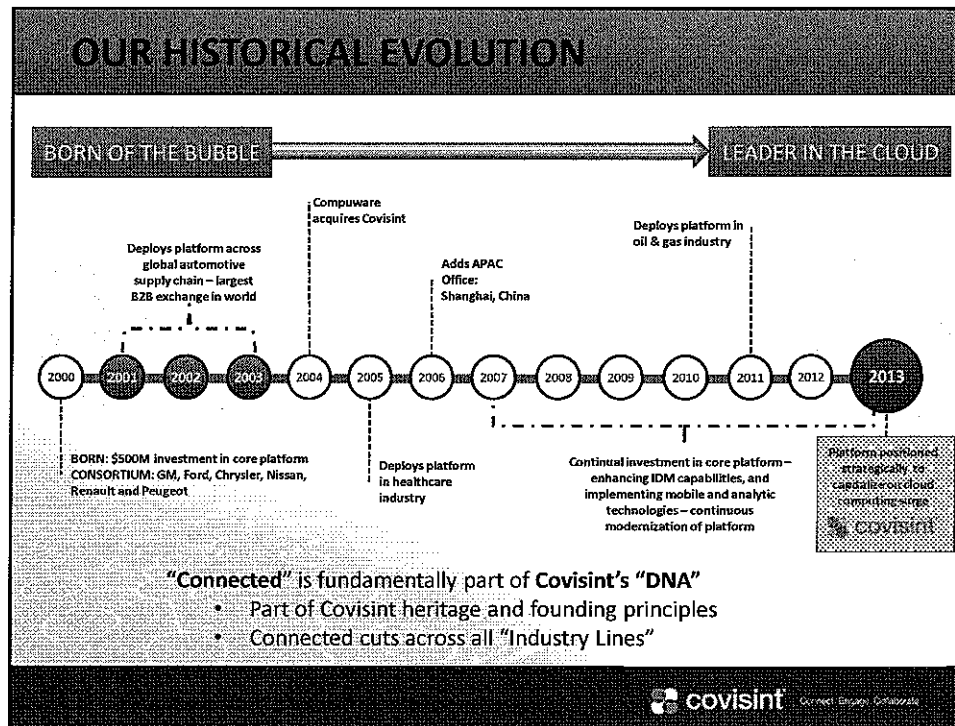
18+ MILLION IDENTITIES

1 BILLION TRANSACTIONS PER YEAR WORLDWIDE



### ONE GLOBAL PLATFORM

**covisint** | Connect. Engage. Collaborate.



## Age old solution



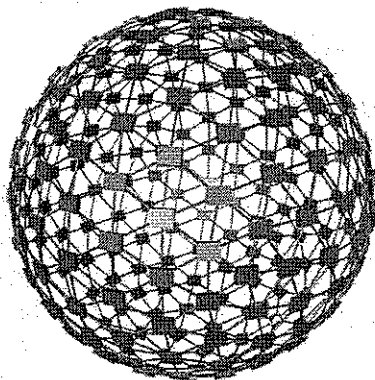
covisint Connect. Engage. Transform.

## Adversarial Innovation



covisint Connect. Engage. Transform.

## Today's Interoperability Mandate



- Outsourcing Providers
- Software on Demand Providers
- Suppliers
- Dealers
- Industry Portals
- Business Customers
- Joint Venture Partners
- Consumers

covisint Connect. Engage. Collaborate.

## Movement Toward Connected World

➤ It started with CE

➤ Quickly led to Connected:

- Automobiles
- Healthcare
- Homes
- Energy
- Manufacturing
- Industries
- Society

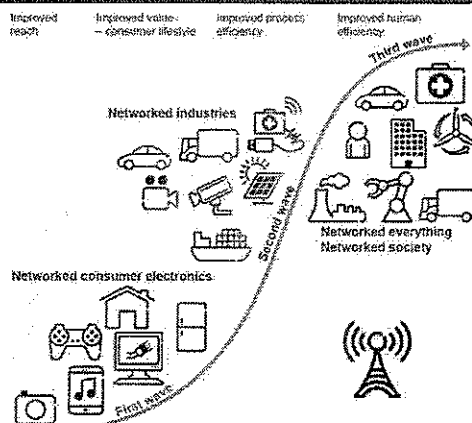


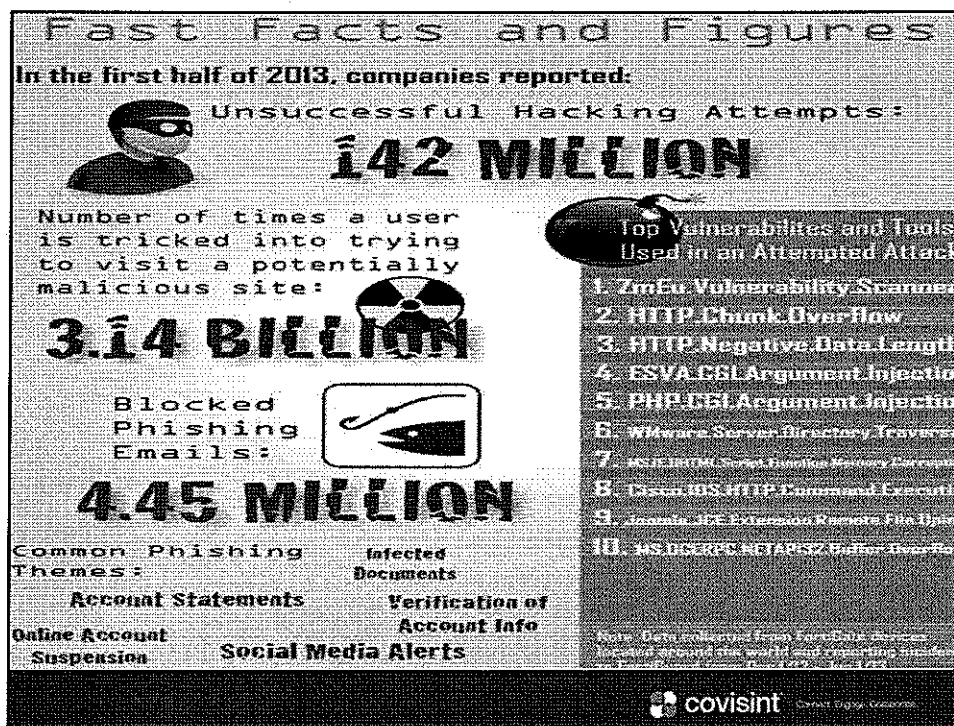
Figure 2: The three waves of connected device development.

Connected is much bigger than Automobiles.

Connected Automobile is part of the "Connected World".


Connected is a new way of life.

covisint Connect. Engage. Collaborate.



## Types of threats

- External threats** that come from the increasing sophistication of cybercrime, state-sponsored espionage, more activism moving online, and attacks on systems that have physical impact in the real world
- Regulatory threats** that come as regulators call for greater transparency about incidents and security preparedness, while increasing requirements for data privacy
- Internal threats** that come as technology introduces new benefits at a relentless pace and the business adopts them without understanding the security risks.


© 2013 Covisint, Inc.

## EXTERNAL THREATS

### 1. Cyber criminality increases as Malspace matures

The sophistication and scale of the global industry that has evolved to commit cybercrime, espionage and other malevolent activity will grow and develop.

### 2. The cyber arms race leads to a cyber cold war

Nations developing more sophisticated ways to attack via cyberspace will get better at it, those who haven't will start, and organisations will suffer collateral damage. Targets for espionage will include anyone whose intellectual property can turn a profit or confer an advantage.

### 3. More causes come online; activists get more active

Anyone not already using the Internet to advance their cause will start: customer affinity groups, community associations, terrorists, dictators, political parties, urban gangs – the list is endless. Online organising will become easier and protest channels will be available to greater numbers.

### 4. Cyberspace gets physical

The increasing convergence of cyber and physical worlds will bring more attacks on physical systems, from attempts to turn out lights or climate control systems to disrupting manufacturing systems. Whether attacks are successful or not, credible publicised threats will cause disruption and panic.

## Magnifiers and Recommendations

### External threat magnifiers include:

- Mobile malware, especially targeting mobile banking
- Attacks on smartphones and internet telephony: eavesdropping on calls and meetings, tracking locations, stealing information
- Domain name abuse from new top level domains and non-latin domain names

### External threat recommendations include:

- Ensure standard security measures are in place
- Develop cyber resilience by establishing a cyber security governance function, timely attack intelligence gathering and sharing, a resilience assessment and adjustment capacity and a comprehensive response plan
- Monitor the threats and share information

## REGULATORY THREATS

1. New requirements shine a light in dark corners, exposing weaknesses. Further movement toward increasingly transparent security disclosures will publicise weaknesses, making organisations more vulnerable to attack. Organisations forced to report security risks may have as much to fear from customers and business partners as they do from hackers and regulators.
2. A focus on privacy distracts from other security efforts. New privacy requirements from consumers, business customers and regulators impose a heavy compliance burden. Organisations will need to decide whether to invest in the necessary security and legal controls, outsource to someone who can, or exit certain markets. They will also need to consider the message their actions send to their customers.



## Magnifiers and Recommendations

Regulatory threat magnifiers include:

- Possible creation of cyber havens: countries providing data hosting without onerous regulations
- Mandate to have real-time reporting, not just an audit snap-shot
- Inadequate security with critical business partners
- Perception that the US monitors everything

Recommended actions include:

- Amend your data protection framework and information management procedures to reflect legislative changes.
- Review new requirements in detail so that, as much as possible, you can align privacy-related controls with other controls, decreasing overhead and increasing effectiveness.
- Join and participate in industry and other associations to assess and influence policy.





## Internal Threats

### 1. Cost pressures stifle critical investment;

An undervalued function can't keep up. Even organisations that are increasing security spend have a legacy of under-investment that can't be corrected overnight. But cyber criminals have been investing, and it will become easier and less expensive to buy criminal technology and services.

### 2. A clouded understanding leads to an outsourced mess

Continued cost pressure will lead to a new form of digital divide: between organisations that understand the marriage between IT and information security – and everyone else. Leading organisations will appreciate the strategic value of channels, systems and information and will invest; the others will suffer competitive disadvantage and heightened risk of damaging incidents.

### 3. New technologies overwhelm

Organisations are unlikely to slow their adoption of new technology or decrease their participation in cyberspace. Along with business benefits come potential vulnerabilities and methods for attack, and organisations will continue to be hit. Organisations that don't understand their dependence on technology may have a nasty surprise if it leads them astray or suddenly goes offline.

### 4. The supply chain springs a leak as the insider threat comes from outside

A modern organisation's data is spread across many parties, and more organisations will fall victim to incidents at suppliers. This will increase as organisations further digitise supply chains, outsource functions and rely on external advisors. 3D printers create three-dimensional products from digital blueprints – increasing the theft of intellectual property, the frequency of attacks and the amount of counterfeit product on the market.

## Magnifiers and Recommendations

### Internal threat magnifiers include:

- Hidden security costs of seemingly attractive business initiatives
- Artificial intelligence decision making used in automated business processes

### Recommended actions include:

- *Raising the game* to help senior management understand the value of information security. Adopt information security governance to raise the game of the information security function and integrate with other risk and governance efforts within the organisation.
- Understand your organisation's risk appetite and ensure the value of continuous security investment meets the business need and is adequate and well spent.
- Take ownership of coordinating the contracting and provisioning of business relationships, including outsourcers, offshorers, supply chain and cloud providers.



